مجلة جامعة الشارقة للعلوم الإنسانية والاجتماعية

جامعة الشارقة
UNIVERSITY OF SHARJAH

University of Sharjah Journal

A Refereed Scientific journal

of

Humanities & Social Sciences

Vol. 19, No. 2
Dhu al-Qadah 1443 A.H. / June 2022 A.D.

ISSN : 1996 - 2339

University of Sharjah Journal for Humanities & Social Sciences, Volume 19, No. 2 June 2022
https//:doi.org/10.36394/jhss/19/2/8

Social Media and Privacy in the UAE: A Survey Research

Abderrahmane Azzi[1]
Samiya Dakhane[2]

Received on: 21-07-2020 **Accepted on: 26-11-2020**

Abstract:

Social media is one of the most important agents of social transformation in modern times. They play a critical role for millions of people. Platforms such as Facebook, Twitter, Instagram, and Snapchat, are used for socializing, posting updates, communicating with friends and family members, as well as sharing photos. The platforms assist individuals in connecting with thousands of people and hence have the potential of influencing people's lives including the potential negative impact of misuse such as re-sharing someone's data without their consent. Social media users are expected to use the social media platforms responsibly as privacy is essential in avoiding harm, distortion, public disclosure, and abuses.

The study investigates privacy in social media from a legal and ethical perspective in the UAE. It addresses the concern of the users who might be oblivious of privacy, data protection guidelines and the gap in research on privacy in social media. The theoretical background is grounded in social utilitarian ethical theory as an ethical framework. The legal theory applies as it defines and sets boundaries for privacy and its different manifestations in social media.

Privacy awareness is a crucial factor in social media websites. The providers of these platforms should have a level of responsibility to guide and enlighten users to take caution and prevent invasion of privacy on

(1) College of Communication - University of Sharjah (Sharjah - U.A.E.)
aazi@sharjah.ac.ae

(2) College of Communication - University of Sharjah (Sharjah - U.A.E.)

their personal information on these websites. The findings of this research paper assist social media users and institutions to be conscious and take precautionary to protect their private information and data.

The Cyber Crimes Law (Federal Law No. 5 of 2012) in the UAE considers violating privacy on social media a civil offense. It punishes the offender with a fine of not less than AED 100,000 but not in the excess of AED 300,000. The majority of social media users are unaware of the methods to protect their personal information shared online as the technology is getting easier and sharing a photo is only one click away, they remain unaware as to how this might affect their lives.

The study indicated that there are many related legal frameworks on online privacy in the UAE. The study shows from an ethical perspective, that the members of the sample do not have enough ethical awareness on the issue of privacy on social media.

While the ethical perspective remains controversial, the legal perspective on the privacy of social media in the UAE is somehow solid, as it is based on many laws that protect the privacy of users; such as the UAE Penal Code and the Cybercrime Law, such regulations are the basis for the emerging laws that are growing due to the evolution of social media systems across the world.

Keywords: privacy, social media, utilitarian ethical theory, legal theory

1.1 Research Problem:

Technology advancement resulting in smartphones and other communication devices supporting the use of social media has transformed the way and amount of information and data shared in the digital era. This is because social media platforms enhance connectivity which, in turn, enables information sharing. Although social media platforms have converted the world into a global village, some legal and ethical frameworks do regulate their usage in terms of data and information sharing [Rajan, Ravikumar, Al Shaer, 2017, p.3]. However, social media usage is a double-edged sword that causes harm to individuals and institutions. This is attributed to the security and privacy of information and data. There is an increase in unauthorized access, sharing, and usage of information as well as the rise of cybercrimes. A report by Bomah (2016) affirmed that the incidents of data breaches increased by 24% in the UAE resulting in a significant loss of personal data. Further, EMC (stands for the founders Richard Egan, Roger Marino & John Curly) (2014) found the cost of downtime experienced by businesses because of data loss was over US$1.7 trillion yearly. The United Arab Emirates has set down wide-ranging rules and regulations that govern media in the region. It has also prohibited different behaviors on social media as well. Article (21) of a decree of the federal law on combating federal information technology crimes stipulates that " Shall be punished by imprisonment of a period of at least six months and a fine, not less than 150,000 Dirhams and not excess of 500,000 Dirhams or either of these two penalties whoever uses a computer network or and electronic information system or any information technology means for the invasion of privacy of another person in other than the cases allowed by the law and by any of the following ways:

1. Eavesdropping, interception, recording, transferring, transmitting, or disclosing conversations or communications, or audio or visual materials.
2. Photographing others or creating, transferring, disclosing, copying or saving electronic photos.
3. Publishing news, electronic photos or photographs, scenes,

comments, statements or information even if true and correct.

Shall also be punished by imprisonment for at least one year and a fine not less than 250,000 Dirhams and not more than 500,000 Dirhams or either of these two penalties whoever uses an electronic information system or any information technology means for amending or processing a record, photo or scene for the purpose of defamation of or offending another person or for attacking or invading his privacy" [Federal Law No. 5 of 2012 on combating cybercrimes].

Apart from the economic losses, there are other losses, including social and psychological sufferings incurred by the victims of privacy breaching and cyber-crimes committed through social media and other platforms.

The UAE's varied arrays of media platforms are well regulated. Article (378) in UAE Penal Code stipulates that "Shall be sentenced to detention and to a fine, whoever violates the private or familial life of individuals, by perpetrating one of the following acts, unless authorized by law, or without the victim's consent:

- If he lends his ears, records or transmits, through an apparatus of any kind, conversations that took place in a private place or through the telephone or any other apparatus.
- Captures or transmits, through any kind of apparatus, the picture of a person in a private place.

Should the acts, referred to in the two preceding paragraphs, be perpetrated during a meeting in front of the attending persons, their consent shall be presumed.

Shall be sentenced to the same penalty, whoever publishes through any means of publicity, news or pictures or comments related to the secrecy of private or familial life of the individuals, even if correct.

Shall be sentenced to detention for a maximum period of seven years and to a fine, the public servant who perpetrates one of the acts mentioned in the present article relies on the strength of the authority of his position.

The apparatuses and other objects that may have been used in perpetrating the crime shall, in all cases, be confiscated and order shall be given to erase all relative recordings and destroy them" [UAE Penal Code, 2011, p. 179].

The Federal Legislator has stressed the penalty for assaulting the privacy of others by using information technology and the Internet, because of the speed of spreading information through the Internet and the inability to control that.

Article (31) of the constitution stipulates that "the freedom and confidentiality of postal and telegraphic communications and other means of communication shall be guaranteed following the law" [United Arab Emirates' Constitution, 1971, p. 8].

1.2 The Significance of the Study

In everyday life, digital platforms and the social web play a significant role in information and communication sharing. Some of the information shared on social media platforms are sensitive and can lead to harm at the individual and societal level. Within the UAE, the utilization of social media is guided by legal provisions including privacy issues treated as a civil tort offense.

The right to privacy is constitutionally guaranteed in the United Arab Emirates. Article 31 of the constitution stipulates that "the freedom and confidentiality of postal and telegraphic communications and other means of communication shall be guaranteed following the law." (Federal Law No.5 of 2012) The article prohibits the sharing of photos, images, or any other pornographic materials against the social norms and acceptable values. As Well states, the law reinforces data privacy including in the social networks [Wells, 2017, p.385]. This research fills the gap in research and assists users and institutions in understanding the importance of privacy awareness, the processes of securing private data and information and the legal and ethical implications of violating the right to privacy. The research assists lawmakers to further examine the legal aspect of the ever-changing practice of violating privacy for individuals and institutions.

1.3 Theoretical Framework:

The right to privacy became an international human right before it was a nationally established fundamental right. The notion was formed years after World War II. Back then, the state constitutions only protected aspects of privacy such as the inviolability of the home and of the correspondence. According to Article 12 of the United National Declaration of Human Rights (UDHR) 1948, "No one shall be subjected to arbitrary, neither with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks" [Universal Declaration of Human Rights, 2015, p.26].

The right to privacy was also included in many constitutions in over 130 countries: Articles 21 of the Arab Charter on Human Rights stipulates that: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to unlawful attacks on his honor and reputation. 2. Everyone has a right to the protection of the law against such interference or attacks" [Arab Charter on Human Rights, 2004, p.155].

Article 8 of the European Convention on Human Rights represents the right to respect private and family life: "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except by the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" [European Convention on Human Rights, 1950, p.10]. Article 11 of the American Convention on Human Rights states: "1. Everyone has the right to have his honor respected and his dignity recognized. 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation. 3. Everyone has the right to the protection of the law against such interference or attacks" [American Convention on Human Rights, 1979, p.148].

The right to privacy has been a subject of international attention, after the global surveillance disclosure of 2013 started by former National Security Agency (NSA) employee Edward Snowden, where he exposed the massive surveillance program of the NSA and the British GCHQ (Government Communications Headquarters) that caused a global outrage [MacAskill, 2019].

In social media, the issue of privacy can be evaluated with the help of utilitarian ethical theory. The theory assumes that the wrongness or rightness of a decision or action is based on whether it will minimize pain and maximize pleasure for the majority of people involved. In social media, this theory would perceive the protection of privacy as a course of action that will support the wellbeing and prevent harm to the user community.

The legal perspective is in line with the premises of this theory as it seeks to protect individuals and institutions from the harm of violating the right of privacy and achieve the wellbeing of society. Users are likely to respect or follow the privacy requirements to avoid the consequences, which involve prison and fines as specified in the law.

What is considered to fall within the right to privacy or deemed to fall outside its scope, varies from time to time and even within one society. That is why there is a lack of a generally accepted definition of privacy.

The theory was developed in the 19th century by Jeremy Bentham and John Steward Mill and is based on the assumption that an ethical decision or action is the one that brings the maximum happiness to most of the people who are concerned [Sheng, 2012, p.25]. The utilitarian ethical approach is based on two criteria or features. Firstly, the approach emphasizes prudential reasoning to determine the means to solve a situation and reach the desired end. The assumption used is that whatever decision or action is taken, the most efficacious means of achieving happiness is right and legitimate [Sheng, 2012, p.26]. The argument is that by doing so, it will be possible to prevent situations that produce greater suffering or pain to the community or the people involved. The ethical approach ensures that pragmatic considerations ratify decision or action.

The utilitarian approach would perceive the protection of privacy in social media as a given course of action that will help to protect society [Sheng, 2012, p.29]. Such can be argued from different perspectives guided by the utilitarian ethical approach. Every individual in any society should have the right to decide about the possession and usage of information about him or her. In other words, every individual has the right to privacy. That means, from a utilitarian perspective, protecting an individual's privacy in social media is ethical. In today's digitized world, social media play an essential role in the lives of people in regards to facilitating effective communication and information sharing. Some of the information shared through social media platforms is very sensitive and can have a significant impact on individuals' lives if shared with a third-party or unintended parties. Besides, information shared on social media can have a negative impact on social, political and economic stability in a community, country or region. Information shared on social media can cause conflict. Bearing this in mind, it is essential to engage an ethical approach in determining the right way to treat the issue of privacy in social media in the UAE.

In any situation that affect many people, it is essential to make decisions that are guided by the considerations of what impact will the decisions have on the welfare interests of the people affected [Mill & Sher, 2002, p.49]. The utilitarian theory can be considered as one of the approaches to guide how the issue of privacy in the UAE that is associated with the use of social media can be solved. The utilitarian framework is therefore appropriate for determining a balanced decision regarding the issue of privacy in social media. The ethical approach can be used by lawmakers in UAE to determine the best legal framework that can solve the issue of privacy in social media. The theory can be used to find a balance between providing people with their fundamental rights and providing them with the needed security. The theory can be used to determine how social media platforms and organizations should be regulated as well as regulating social media users with regard to protecting individuals' privacy in social media platforms.

The issue of privacy also occupies an important position in Islamic tradition Qur'an and Sunnah (Hadith). Islam asserts the importance of the

fundamental human right to privacy. Some verses from the Holy Quran are evident to that. "Do not spy on one another" (49:12); "Do not enter any houses except your own homes unless you are sure of their occupants' consent" (24:27). The explanation or this verse according to Tafsir Tabari underlined that person is prohibited to enter the other's home if he/she does not have consent from the owners. Tabari assured the importance of greetings (salam) before entering someone's property either by stating the greeting words or by knocking door three times together with greetings as a respected approach to permission from the owner [Lubis M, Kartiwi M, 2013, p.2].

1.4 Legal Context:

The Penal Code in UAE requires those with access to people's information not to disclose or publish that information. It prohibits individuals from publishing people's private affairs and further requires that those who violate the code of imprisonment or fine. Based on this law, therefore, individuals who publish information that is supposed to be treated as a private affair of other people are supposed to be imprisoned or fined. The same provision can be used to solve privacy issues in social media. The Penal Code can be used to argue that corporate entities can be liable for the use of individuals' information that involves disclosure or sale for monetary purposes.

The constitution of the UAE addresses the issue of privacy by indicating that individuals have the freedom to communicate and secrecy [MacCuish & Dandekar, 2016]. In other words, people are free to share information and also to have secrecy or privacy of their information. The provision can be argued that it was intended to give individuals the right to privacy with regard to their personal affairs. The same argument can be used when addressing the issue of privacy on social media. Using this provision, it can be argued that all individuals have a constitutional right to the privacy of their communication and information on social media. Invasion of individuals' privacy on social media may, therefore, translate to "wrong act" or "illegality". According to the Civil Code, a person whose rights to privacy have been infringed has the right to demand such infringement to stop and to demand compensation. Further, wrongful invasion of

an individual's right to privacy may give rise to a call for civil action against the violator for damages caused. The Civil Code requires that the perpetrator should rectify any damage that is caused by the invasion of privacy to a victim. Privacy can, therefore, be considered a constitutional right. Therefore, every individual in the UAE is provided with the right to privacy by the constitution [The UAE Data Protection Law, 2019].

The cybercrime law is a legal provision that can be used to solve the issue of privacy in social media in UAE. The Federal Law No. 5 of 2012 focuses on the misuse or abuse of electronic information [Khaleej Times, 2016]. The legal framework deals with identity theft, hacking, and fraud. Cybercrime law makes it illegal for anyone to disclose individuals' private information without owners' authorization. The law, therefore, can be considered relevant when discussing the issue of privacy in social media and how to address the issue from the legal perspective [Saleem S, 2013].

The UAE constitution can, therefore, be used to determine the best to solve the issue of privacy on social media from a legal perspective. The lawmakers can use provisions like Article 36 that states: "Homes shall be inviolable. They may not be entered without permission on from their inhabitants except in accordance with the provisions of the law, and in circumstances laid down therein" to determine how to address privacy in social media [The UAE Constitution, 2004]. Such provisions on the constitution can also be used to determine how issues relating to the violation of individual's privacy on social media are addressed from a legal perspective. Although no legal provision specifically addresses the issue of privacy on social media, the existing provisions can be used to guide how to address the issue. The provisions on the UAE constitutions are therefore relevant for achieving the objectives of the proposed study.

The legal perspective is triggered by the need to impose protection of private information and control the use of social media. The perspective focuses on laws and policies enacted with the aim of protecting individuals from firms, governments and other persons against the breach of privacy and its subsequent costs. The legal provisions like Article 379 of the UAE Penal Code provide guidelines to the online social network users and providers

The main UAE Law that is related to privacy protection in the UAE Constitution is Article 36 that stipulates that: "Homes shall be inviolable. They may not be entered without permission from their inhabitants except in accordance with the provisions of the law, and in circumstances laid down therein" [The UAE Constitution, 2004]; The Legal Code in Article 379 that stipulates: "Shall be sentenced to detention for a minimum period of one year and/or to a minimum fine of 20,000 Dirhams, whoever by virtue of his profession, craft, position or art is entrusted with a secret and divulge it in cases other than those allowed by law or if used for his own personal interest or for the interest of another person, unless authorized by the confiding person to disclose or use it. The penalty shall be imprisonment for a term not exceeding five years just in case the perpetrator may be a public servant or a person in charge of a public service who was confided the secret or on the occasion of discharging his duties or performing his service" [The UAE Penal Code, 2011, p. 180]. Cybercrimes Law in Article 21 stipulates the following: "Shall be punished by imprisonment of a period of at least six months and a fine not less than 150,000 Dirhams and not in excess of 500,000 Dirhams or either of those two penalties whoever uses a computer network or and electronic information system or any information technology means for the invasion of privacy of another person in aside from the cases allowed by the law and by any of the subsequent ways: 1- Eavesdropping, interception, recording, transferring, transmitting or disclosure of conversations or communications, or audio or visual materials. 2- Photographing others or creating, transferring, disclosing, copying or saving electronic photos. 3- Publishing news, electronic photos or photographs, scenes, comments, statements or information though if true and right. Shall be punished by imprisonment for a period of at least one year and a fine not less than 250,000 Dirhams and not more than 500,000 Dirhams or either of these two penalties whoever uses an electronic information system or any information technology means for amending or processing a record, photo or scene for the purpose of defamation of or offending another person or for attacking or invading his privacy" [Federal Decree Law no (5) of 2012, 2012, p. 5].

In the United States, there are several laws that touch on social media privacy, internet and data security issues, but with arguments that the

1974 Privacy Act is the foundation for it all [US Norton]. Laws are: Cyber Intelligence Sharing and Protection Act (CISPA), Children's Online Privacy Protection Act (COPPA), Electronic Communication Privacy Act (EPCA) and Computer Fraud and Abuse Act (CFAA). The CFAA makes it a crime to access and share protected information and therefore it examines federal laws connected to computer crimes.

California for instance, has both the criminal and. civil invasion of privacy laws. The Penal Code of California criminalizes a person who invades someone else's privacy. The law involves using a device to view someone inside a private room or secretly photographing a person's body under the clothing for sexual arousal or secretly recording or photographing someone in a private room to view that person's body.

In civil invasion of privacy cases, the act of invading the privacy of another is called "tort", or a legal wrong that damages another person. Whoever suffers from damages can file a lawsuit in court for the harm done to him, his reputation or his business [SCLG, 2018].

Article 8 of the European Convention on Human Rights presents the right to privacy in the United Kingdom; it stipulates: "Everyone has the right to respect for his private and family life, his home and his correspondence". UK laws defend the privacy of individuals on social media. However, there are a lot of exclusions which allow privacy to be breached when there is a benefit to the society [Baker, 2016]. Those privacy laws will not only be challenging to state in court, but will also be tough to implement on the internet. Many people have actually argued that current UK privacy laws are old-fashioned in light of the internet age [Rankin, the Lawyer Portal]. But on April 8, 2019, a press release on the GOV.UK mentioned that the government has announced tough new measures to ensure the UK is the safest place in the world to be online [2019].

The invasion of privacy although it may vary between considering it a civil offense or a criminal offense based on the law of a specific country but the issue of invasion of privacy is recognized as a subject that needs to be determined within the law both in Arab & West countries.

1.4 Research Aim and Objectives:

The primary aim of the research is to investigate social media and the issue of privacy in the UAE while focusing on ethical and legal perspectives. The current study would strive to achieve six objectives:

1. Examine the ethical dimension of privacy in social media.
2. Legal aspects of privacy of social media in the United Arab Emirates.
3. Assess the extent to which social media users in the UAE have ethical awareness in their dealing with social media.
4. Assess the compliance level among social media users to the privacy policy set in place by the social media platforms.

1.5 Research Questions

1. What are the ethical considerations of privacy in social media in the UAE?
2. What are the legal provisions on privacy in UAE?
3. What is the level of ethical awareness of privacy in social media users in the UAE?
4. What is the compliance level among social media users to the privacy policy?

2.0 Literature Review:

Privacy is an old concept that traces its roots in philosophical discussions, the most popular being the attempt by Aristotle to distinguish between the public sphere of the polis and the private sphere of Oikos [DeCew, 2018, p.14]. The privacy of individuals is also taken away when unauthorized individuals get access to identifying information. However, the description can only be applied in physical privacy. Regarding information privacy, violation of privacy involves the disclosure of personal information that has a negative impact on individuals identified by the information. To most individuals, the issue of privacy is interpreted in relation to the exposure

of photos of an individual's body to others [DeCew, 2018, p.17]. However, themes of privacy are shared, and therefore the idea of what is private to many people varies. To many, private refers to that which is sensitive to individuals [DeCew, 2018, p.18]. The best way to determine the meaning of privacy is to consider concepts. Some of the common concepts used include secrecy, right to be let alone, states of privacy, right to limit access to personal information, autonomy and personhood, protection of intimate relationships, and self-identity [Rengel, 2013, p.53].

The term privacy is used to describe the ability of an individual or a group to protect or seclude their information and data. It is about having the right to private life free from invasion. As noted earlier, privacy is described as the "right to be let alone," meaning that every individual has the right to opt for seclusion from others or the right to seek immunity from being observed by others in a private setting [Rengel, 2013, p.65]. Finn, Wright, and Friedewald (2013) argued that the term (privacy) is mostly used to critique technological applications but still there is no clear description of what security entails. This is because definitions are influenced by different contexts and experiences. Therefore, it is difficult to have a universal definition. Also, privacy violation involves the disclosure of personal information without the authority of the individual identified by the information [Rengel, 2013, p.69]. There are also different ways in which privacy can be violated depending on the individuals' understanding and contexts including intrusion into the person's affairs or private setting [Finn, Wright, Friedewald, 2013, p.6]. This simply involves intruding individual's wish for solitude.

A number of scholars trace the origin of the concept to privacy law developed in the 1890s in America. The law indicated that information privacy goes beyond modesty of addressing the issues relating to rights to information about the self [Rengel, 2013, p.79]. In some cases, privacy is concerned with data stored in digital formats, and that can be linked to individuals. The main concern relates to who has the access right to such data and the right of the owner to control access to the data [Jøsang, Maseng, Knapskog, 2009, p.209]. Privacy differs among individuals and cultures, and scholars provided different definitions. For this study,

privacy refers to the publication of private facts like names, photos, date of birth, bank account number or any information about someone's personal life that has not been previously revealed to the public, intrusion into secluded data systems without authorization like watching, listening to and recording another person's private activities, usage of the personal data of an entity without permission like reposting a personal picture or video of an individual without their consent.

A study by Virpi Tuunainen and Olli Pitkanen on the user's awareness of privacy on Facebook indicated that most of the active respondents on Facebook reveal a considerable amount of private information [Tuunainen, Pitkanen, Hovi, 2009, p. 9]. Against their own certainty, they are not aware of the visibility of their information to people they do not necessarily know. The users, who are mostly young adults, do not have significant privacy concerns yet they claim they have enough knowledge of privacy risks.

A study by Pew Research Center found that 91% of Americans "agree" or "strongly agree" that people have lost control over how personal information is collected and used by all kinds of units [Madden, 2014, p. 6]. While privacy on social media can have different explanations, a study by Web Foundation presented that the term "Privacy on social media" for teenagers is their "ability to control their situation, including their environment, how they are perceived, and the information that they share" [Marwick, Boyd, 2014, p.1056].

Another study published in Pew Research Center's Internet & American Life Project by Mary Madden found that social media users have some difficulty in managing privacy controls despite the educational background. The social media privacy settings and its complexity differs between different platforms yet they are constantly working to change the default settings over time. The study shown also that despite this lack of managing their privacy on social networks, profile owners have become more active managers of their profile than before, which mean they are more familiar nowadays with other options to protect their privacy through deleting unwanted friends or removing content which they no longer interested in posting it [Madden, 2012, p.8].

Another study suggested that privacy may be attacked in a few ways if personal information shared online is not used reasonably and dependably. This means if the proper information strategies and practices provide people with control over the utilization of their own information, protection concerns can be intervened. The study pointed out to the advancement of trust in an online domain and considered it as unpredictable on the ground that the online world is characterized as fragile. And that is the reason why many studies focused on the inclination of users to unveil data on the premise of both trust and protection [Senthil Kumar, Saravanakumar, Deepa 2016, p.118].

A research work from Web Foundation (2017) has pointed out the importance of governments authorizing regulations that protect the data shared online. The same research also highlighted that with the exception of the EU's General Data Protection Regulation (GDPR), people in most countries are not protected by solid monitoring outlines.

2.1 Main Concepts:

Privacy: Although there have been a lot of attempts to define "Privacy", the notion has proved to be very difficult to define. As Serge Gutwirth says, "The notion of privacy remains out of the grasp of every academic chasing it, even when it is concerned by such additional modifiers as "our" privacy, it still finds a way to remain elusive" [Finn, Wright, 2013, p.2]. However, privacy can be identified as the right of individuals or groups or institutions to decide when and where the personal information is accessible by other parties. There are four types for the invasion of privacy: False light which means invading a person's privacy by involving something untrue about him or her; Appropriation means using an individual's name in an advertisement or a commercial without their consent; Public Disclosure which refers to the true information of an individual's life that would be offensive to the person if it becomes public; and Intrusion which the research topic focuses on.

Social Media: Digital web platforms are used for information sharing and socialization [Cross & Shimonski, 2014, p.256]. It consists of Facebook, Twitter, Instagram, YouTube, SnapChat and many other platforms used by users to communicate and share information with other parties.

In the current world, social media have been substantially used as a means of communication. In light of this, there is a need to enhance the social media security approach. The aim of the strategy is to give people the capacity to do what's needed without compromising security. Therefore, one needs to understand what security is and how security will be achieved [Cross & Shimonski, 2014, p.257].

Ethics: Acceptable behavior or the standard used in defining right conduct and morality [Driver, 2014, p.186]. In other words, it regards to principles and values upheld to guide one's behavior and conduct. Nevertheless, ethics play a vital role in structuring, defending and recommending concepts of wrong and right behavior.

Law: The system of rules applied in a society or community to define behavior and demonstrate how people are governed or interrelate as imposed by the authorities within the jurisdiction [Kantorowics, 2014, p.157]. Law is significantly utilized as a means of setting out guidelines that need to be critically observed. Additionally, it is critically used in the control of conduct among individuals.

3.0 Methodology:

The research methodology involves a survey asking social media users about issues of privacy related to social media usage.

Context for Practical Study:

An 'institution-based quantitative cross-sectional' study was conducted at five universities in the United Arab Emirates (UAE), a region with an array of universities that attracts both local and international academic communities. The study period was from February to April, 2019.

Participants:

A sample of 150 participants comprising of 120 students and 30 professors from five universities situated in the UAE was selected arbitrarily. The institutions are the University of Sharjah, Hamdan Bin Mohammed Smart University, Al Ain University, New York University in Abu Dhabi and Ajman University. The universities are selected to give

a broad understanding of how students in institutions of higher learning approach privacy in social media.

A stratified sampling technique was employed to select the participants from the five listed universities, based on availability. The sample is arbitrary. In total, a sample size of 50 students and 30 professors were arbitrarily selected. Other than the two categories, 70 visitors to campuses were involved from the five universities.

Table (1): Sample of Characteristics

Variable	Participants	Percentage
Gender		
Male	71	47.3%
Female	79	52.7%
Participants		
Professors	30	20%
Students	120	80%
Age		
25-35	46	30.7%
22-25	31	20.7%
36-47	25	16.7%
16-18	14	9.3%
46-55	9	6%
Above 56	7	4.7%
Education		
University Students	67	44.7%
Postgraduates	55	36.7%

High School Students	22	14.7%
Secondary Students	6	4%
Social Media Account		
Have a social media account	147	98%
Doesn't have a social media account	3	2%

Method: Data Collection Procedure and Tool:

The study is a survey research. The sample consists of students, professors and visitors to these five universities: the University of Sharjah, Hamadan Bin Mohammed Smart University, Al Ain University, New York University and Ajman University. The sample is (150) was selected arbitrarily based on availability.

The participants were reached through various methods such as receiving hard copies, phone calls and emails. The questionnaire was emailed to 50 students and 30 professors. The rest 70 (students and visitors; who were mostly to-be enrolled students) received a hard copy. The first part of the questionnaire collected general information of the students, professors, and visitors. The second part addressed privacy issues attached to social media. Prior to participating, anonymity was assured.

Validity and Reliability:

The study problem, questions and questionnaire were submitted to a panel of 3 reviewers (faculty) from the College of Mass Communication at the University of Sharjah who found that most of the questions are consistent with a few modifications. A pre-test conducted among 20 students at the University of Sharjah assured data quality. After the pre-test analysis, necessary changes were made before the collection of actual data. In the first pre-test, two samples of open-ended questions were presented. The students did not answer the first attempt of the survey. Consequently,

the two questions: 1. How do social media in UAE guarantee privacy to the users for the information they post online?, 2. List some of the privacy policies that social media are obligated to, were deleted due to the lack of knowledge of the social media users before distributing the final survey.

4.0 RESULT

Part I: General Results

Table 2 - How Long Have You Been Using Social Media Account

Duration of Using Social Media Account		
	Frequency	Percent
More than 6 years	55	36.7
years 5-6	47	31.3
years 3-4	36	24.0
years 1-2	5	3.3
months 1-5	4	2.7
months 6-12	3	2.0
Total	150	100.0

According to (Table 2), the usage of social networking sites has "more than six years" as the highest rate with 36.7 % and 2% of using the social media between 6 – 12 months as the lowest rate. With the fast track of new technology and its involvement in our daily basis life, individuals tend to dive into the virtual life in general and social media in specific to follow up on whatever is coming their way, whether it is education or career.

Although there are many new platforms that appear every day, Facebook is still the favorite social media with 20.3% of the participants, while Flickr is the least engaged with 0.7% since it's uncommon to use here in the Middle East and Gulf countries.

The average time spent on social media every day by the individual falls in several ranges. For half an hour, it is 6.7 %, for 1-2 hours it is 21.3 %, for 3-5 hours it is 43.3%, and for 6-8 hours it is 24.7%, and for more than 9 hours it is 4%.

Part II: Ethical Consideration

Table 3 – How Secure the Data Shared are

Awareness Range on How Secure the Data Shared is		
	Frequency	Percent
Aware	87	58.0
Not concerned	34	22.7
Not aware	29	19.3
Total	150	100.0

In (Table 3), around 58% said that they know about the security awareness on sharing their individual information. Going through the process of signing up for a new digital platform gives you the opportunity to explore how your data will be secured using a specific platform. This means that individuals should read the privacy policies very carefully. However, those who are not aware (19.3%) of this matter could face many challenges with their minimum knowledge of what is secured and what is not and could lead to serious issues in the future. For the query "On a scale of 1-10, rate the social media use in terms of ethical compliance with one being the lowest level of compliance and ten the highest level of compliance", the result obtained is as follows:

Table 4 - Rate of Social Media in Terms of Ethical Compliance

Social Media Use in terms of Ethical Compliance by the Users		
	Frequency	Percent
10	38	25.3
7	32	21.3
8	28	18.7
6	14	9.3
9	12	8.0
5	11	7.3
4	7	4.7
3	4	2.7
2	4	2.7
Total	150	100.0

Part III: Legal Considerations while Using Social Media

Table 5 - Privacy and Ethical Policy on Social Media Sites

Privacy and Ethical Policy		
	Frequency	Percent
Ignore	47	31.3
Read but not fully understand	46	30.7
Skip	37	24.7
Read and understand	20	13.3
Total	150	100.0

Digital platforms tend to introduce the user to its terms of use and policies before they join the platform. The first stage in creating any account on one of the social media platforms requires the user to read and agree on the terms of use and policies. And the importance of this phase goes to the point that the user cannot proceed with creating the account until they click the agreement. However, the highest rate in the survey (31.3%) is from participants who completely ignored the part without reading policies before signing up and didn't proceed with the signing up. I believe the option "Accept Terms of Use" should be one option from two. The other should be "I have read the Term of Use". Because such difference will allow the Social Media providers to demonstrate that the users who chose to register on their platform are fully aware of all their policies which is not right. Some privacy professionals pointed out that these kinds of consents collecting might not be valid which agree to my argument [Lee, 2016].

Table 6 – Personal Information Held Private & Confidential

Personal Information Should be Held Private and Confidential		
	Frequency	Percent
I strongly agree	61	40.7
I agree	46	30.7
Neutral	21	14.0
I disagree	16	10.7
I strongly disagree	6	4.0
Total	150	100.0

For the query, "Your personal information will be held private and confidential and will not be exposed to the third party 40.7% strongly agreed (Table 6). But I think the reason behind the strong agreement of this statement is because people are confused about which personal information is private, confidential and really important to keep safe. For example, someone might post a picture of their passport and travel ticket online to show their excitement about an upcoming trip and that definitely look very

risk-free act. But with the new technology and applications all over the internet, a lot can be done from just a picture of a passport. And the same goes to any other documents that might seem harmless to post images of like the driving license, marriage certifications or medical records.

Part IV: User's Level of Awareness about their Online Information:

The most important personal information according to the users (Table 7) states that financial Information is very significant to be shared online with a rate of 17.5%. In addition to that, home address, passports license, gender and mobile number are considered the most important personal information according to 66.9% of the participants. (66.9%)

Table 7 – The Most Important Personal Information According to Users

The Most **Important Personal Information According to Users**				
N		Responses		Percent of Cases
		Percent		
Q23[a]	Financial Information	111	17.5%	74.5%
	Home Address	93	14.7%	62.4%
	Passports License	80	12.6%	53.7%
	Gender	71	11.2%	47.7%
	Mobile Number	69	10.9%	46.3%
	Photo	58	9.2%	38.9%
	Biometrics	53	8.4%	35.6%
	Family Members	31	4.9%	20.8%
	Name	21	3.3%	14.1%
	Friends List	20	3.2%	13.4%
	Medical Information	14	2.2%	9.4%
	Nationality	6	0.9%	4.0%
	Work History	6	0.9%	4.0%
Total		633	100.0%	424.8%

Part V: Impact of Violating Privacy on Individual

Table 8 – The Role of the Government in Protecting the Users' Privacy

The Role of the Government in Protecting the Users' Privacy		
	Frequency	Percent
I strongly agree	87	58.0
I agree	47	31.3
Neutral	13	8.7
I disagree	3	2.0
Total	150	100.0

According to (Table 8), 58% agree that the government plays a significant role in protecting the user's privacy but 2% disagree with that. In a statement from the Facebook Co-founder and CEO, Mark Zuckerberg last year, He called for government regulation of the internet. He involves new laws in four areas: "harmful content, election integrity, privacy and data portability". The announcement comes two weeks after a gunman used the site to livestream his attack on a mosque in Christchurch, New Zealand. "Lawmakers often tell me we've an excessive amount of power over speech, and admittedly I agree" said Zuckerberg who added that Facebook was "creating an independent body so people can appeal our decisions" about whatever should be posted or taken down (Afoko, 2019). But will that be possible taking into consideration the variety of websites and social media platforms around the world? An implementation of what's called "Co-Regulation" can be done. It is a kind of cooperation between regulations set by social media providers and the government of each country. This will lead to creating a balance between saving the providers' effort and protecting the user's privacy in the virtual life.

Table 9 – The Role of Service Providers in Protecting the User's Privacy

The Role of Service Providers in Protecting the User's Privacy		
	Frequency	Percent
I strongly agree	89	59.3
I agree	41	27.3
Neutral	11	7.3
I disagree	7	4.7
I strongly disagree	2	1.3
Total	150	100.0

Along with the government, the service providers also play a significant role (Table 9). Around 59% of the participants in the questionnaire agree strongly to this state. Service providers must keep in mind that using social media sites is easy and available to everyone despite their educational and knowledge background. Therefore, their role in protecting the user's privacy is mandatory to every user. Though for those who disagree with this statement (1.3%), I suppose the reason comes from the fact that they trust they are responsible for their safety and privacy online by choosing what, when and where to share their personal information.

Part VI Possibility of Privacy with the Internet

When participants were asked if having more followers on their social media accounts is risky or not, 54.7% agreed it is not and 45.3% said that having more followers is risky (Table 10). In order to evaluate the risk of getting more or fewer followers, we should consider whether these followers are bought or are genuinely earned through what individuals post on their social media walls and the quality of these posts. Some websites which offer the option to buy more followers, such as Instagram, can eventually put the user at danger by asking to provide their email address and sometimes the password of their social media account which may lead to fast access to their personal information.

Table 10 – Risk of Having More Followers

Risk of Having More Followers		
	Frequency	Percent
No	82	54.7
Yes	68	45.3
Total	150	100.0

Generally, social media platforms are an incredible tool sustaining new trends and technological advancements every day. According to (Table 11), 69.3% of the participants in the survey say that it is not obligatory to connect with everyone through social media while 30.7% disagree with that. Although one of the advantages of social media is worldwide connectivity, especially in sites like Facebook, Twitter, Instagram etc., it exposes individuals to harassment, inappropriate contact from others, risk of fraud or identity theft and many other dangers. Those who disagreed with the above statement may consider connecting only with those who are they familiar with in real life or met in real life, which may reduce the risk they will face connecting with different unknown individuals from around the world.

Table 11 – Get Connected with Everyone

Get Connected with Everyone		
	Frequency	Percent
No	104	69.3
Yes	46	30.7
Total	150	100.0

4.1 Summary of Findings

The study has answered the study questions as follows:

- **QUESTION 1:**

The analysis of the literature review and the results suggest that achieving a satisfactory level of privacy is very challenging on social media and probably require more effort from individuals. The majority of users of social media are unaware of the method to shrink the level of vulnerability of their personal data. Therefore, it is the social network platforms' duty to educate users of the risk of contributing in social media. This statement agrees with philosopher Immanuel Kant's assertion: "Do unto others as you have them do unto you" can be applied universally and should direct human interactions. The prophet (ﷺ) said: "None of you will have faith till he wishes for his (Muslim) brother what he likes for himself" [Sahih Al Bukhari 13]. If users and social media owners followed these principles, the awareness of how to protect your privacy and reduce the incidents of privacy invasion will increase which will show major growth in security, which confirms the utilitarian ethical theory that the wrongness or rightness of a decision or action is based on whether it will minimize pain and maximize pleasure for the majority of people involved.

"Privacy is strongly related to trust". If social media developers are willing to share how they control someone's personal information, they can use this to help build trust between the website owners and the users, which eventually will ease the worries over being able to trust each other. The findings state that the majority of the profiles are accessible to the public, which indicates that the privacy setting provided is weak and this enables attackers to hack the profiles and access the information. Based on the state's privacy, the sharing of information by a third party is determined to be a significant ethical consideration.

- **QUESTION 2:**

The protection of personal information and privacy considerations are more important than ever due to globalization and technological development. The privacy on social media in the UAE is protected by the

UAE Constitution in Articles (31), (33) and (36), the Penal Code in Article 379 and the Cyber Crimes Law.

The study found that the state of privacy in the UAE in social media is covered by many branches of law in the UAE, such as the Cyber Crimes Law and the Penal Code to protect individuals and entities from behavior on social media that violate their rights. The Cyber Crimes Law (Federal Law No. 5 of 2012) considers it an offence to use technology to break someone else's privacy, involving taking pictures of others or publishing or displaying those pictures. The UAE Penal Code (Federal Law No 3 of 1987) also considers it an offense to spread someone's photograph without their consent. Therefore, social media users should be very careful to maintain an expected behavior under the UAE law on social media, as it can affect both the offender and those on the receiving end. Although social media platforms are upgraded every day, the UAE authorities are very keen to protect the privacy rights of every resident on its territory.

- **QUESTION 3:**

Even though the social media platforms make it a mandatory to accept the Terms of Use and Privacy Policy, most users do not read or go through these policies and regulations due to the length and complexity of words, especially because not all social media users come from an educational background and knowledge to such important policies which will cause an issue for their own safety and their personal information in the future. Some users might not be familiar with their breaking of legal provisions on privacy in social media simply because they were not aware of such issue mentioned in the Privacy Policy when signing up in a platform. This means that the developers can use such consent by the user to defend against whatever the user committed unwillingly.

- **QUESTION 4:**

The level of compliance among social media users to privacy policy is rather high taking into considerations that the users are open to any regulations and policies that will protect their personal information through the social media platforms. Thus, the findings show that most of the participants are active on one of the social media platforms and ignore

the importance of preventing their profiles from attackers. However, the findings will help social media users and institutions to analyze the significance of the integration of defensive features on the networks to protect their private information and data.

5.0 The Implications of This Research:

The proposed study is supposed to focus on the increasing concerns regarding privacy and data protection issues in social media. The number of individuals and institutions using social media platforms in the UAE has been increasing, and therefore it is essential to conduct a study on the issue of privacy in social media. The study will, thus, help to close the gap existing in research regarding issues of privacy and data protection in social media. It will provide essential insights to individuals and organizations on the importance and to protect private information. The study will also provide essential findings that can be used by lawmakers to structure a necessary legal framework that can address privacy issues in social media.

Most importantly, the study findings will provide an essential foundation for future studies regarding privacy issues in social media to researchers and scholars. The findings will be necessary for scholars interested in studying privacy and data protection issues in social media. They will also be relevant to the legal scholars studying legal frameworks on data protection and privacy in social media.

The study results have strengthened the basic theoretical assumption of ethical theory in that privacy is a major right and principle to be preserved for the wellbeing of society. The study has found however that ethical awareness of privacy among users is not highly present. The reality of social media users indicates the gap between what ought to be and the actual practice of privacy.

6.0 Conclusion:

The investigation on social media and the issue of privacy in the UAE while focusing on the ethical and legal perspective and the effect of privacy in social media in the UAE further examined the moral dimension

of privacy in social media. Based on the research outcome, privacy can be identified as the right of individuals or groups or institutions to decide when, where, and how far their personal information can reach other parties. Personal privacy is attached to one's own life, which is opposite to public life. Privacy is an essential right, to every individual, considered by international constitutions and charters which the national legalization have criminalized its action like capturing images of other individuals in a private place without their consent or recording conversation or overhearing or transferring discussions that were held in a secluded location with any tool or spreading news or electronic images or private information about an individual.

The issue of privacy in social media was analyzed using the utilitarian ethical framework and legal theory.

In UAE, privacy reinforcement can be attained in social terms, particularly when a group of social media users comes up with norms on privacy to be observed. The issue of privacy can also be solved based on the Penal Code in the UAE constitution. The research will assist lawmakers in the constant expansion of the applicable legal framework for the developers of the platform to integrate innovative features to overcome privacy issues. New guidelines must be set in the present legal system on the technical specifications to assist in the control of the sharing and disclosure of private data. Lawmakers can use provisions of the constitution to determine how to address privacy in social media. There is a need to determine how social media platforms and organizations should be regulated as well as regulating social media users regarding protecting individuals' privacy in social media platforms. Privacy awareness is a critical aspect influencing whether privacy is upheld in the use of social media platforms. The online media users must be required to have both the theoretical and practical awareness in order to take caution and prevent the lack of data privacy. Social network websites providers should take the responsibility of enlightening the user. Although there is no explicit legal framework in UAE that addresses specifically the issue of privacy in social media, several laws are relevant. Social media platforms differ concerning the levels of privacy that they provide to their users. It can also be argued that different social media

offers different privacy with different characteristics. There is a need for further exploration of privacy and set new legal dimensions so that the privacy rights of an individual are protected. Social media platforms are constantly improving their features to protect users against privacy issues. Such features include the ability to report content that the user sees as a threat to his/her privacy and easy access to such feature. The developers will then study the reported case and take the necessary measures either by deleting the content, warning the offending user or temporarily or permanently suspending the account. The reasons behind this continuous improvement in such features are due to the error gaps created by the developers themselves or through so-called hackers and to gain the trust of the user to continue experiencing the platform.

References:

Akram, W., & Kumar, R (2017). A study on positive and negative effects of social media on society. *International Journal of Computer Sciences and Engineering, 5*(1), 351-354. https://doi.org/10.26438/ijcse/v5i10.351354

Cross, M., & Shimonski, R. (2014). *Social media security: Leveraging social networking while mitigating risk*. Elsevier. https://doi.org/10.1016/B978-1-59749-986-6.00010-2

DeCew, J. W. (2018). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press. Available at: https://wmich.edu/sites/default/files/attachments/u58/2015/ethics-privacy_info_tech.pdf. Assessed May 14, 2020.

Driver, J. (2013). *Ethics: The Fundamentals*. Wiley.

Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. *European Data Protection: Coming of Age, 1*-27.

https://doi.org/10.1007/978-94-007-5170-5_1

Herschel, R. & Miori, V. M. (2017). Ethics & big data. *Technology in Society, 49*, 31-36. https://doi.org/10.1016/j.techsoc.2017.03.003

Jøsang, Audun, Maseng, Torleiv, Knapskog, Svein J. (2009). Identity and privacy in the internet age. *14th Nordic Conference on Secure IT Systems*, NordSec 2009, Oslo, Norway, 14-16 October 2009. Springer Science & Business Media. https://doi.org/10.1007/978-3-642-04766-4

Kantorowicz, H. (2014). *The definition of law*. Cambridge University Press.

Lee, P. (2016). The nuance of "accepting" vs. "reading" a privacy policy. Retrieved from: https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/the-nuance-of-accepting-vs-reading-a-privacy-policy

Navarro-Arribas, G., & Torra, V. (2014). *Advanced research in data privacy*. Springer. https://doi.org/10.1007/978-3-319-09885-2_1

Rajan, A. V., Ravikumar, R., & Al Shaer, M. (2017). UAE cybercrime law and cybercrimes: an analysis. in cyber security and protection of digital services. *International conference on cyber security.* https://doi.org/10.1109/CyberSecPODS.2017.8074858

Rengel, A. (2013). *Privacy in the 21st Century*. Martinus Nijhoff Publishers. https://doi.org/10.1163/9789004192195

Siddiqui, S., & Singh, T. (2016). Social Media its impact with positive and negative aspects. *International Journal of Computer Applications Technology and Research, 5*(2), 71-75. https://doi.org/10.7753/IJCATR0502.1006

The UAE Federal Cybercrime Law No. 5 of 2012.

Young, B. J. (2014). A comparative study of the legal frameworks and protection of digital content in the United Arab Emirates and Australia to the practice of blocking digital content based on location (geo-blocking) and its associated circumvention technologies. *International Journal of Journalism & Mass Communication. 1*(11). https://doi.org/10.15344/2349-2635/2014/101

وسائل التواصل الاجتماعي والخصوصية في دولة الإمارات العربية المتحدة: بحث ميداني

عبد الرحمن عزي[1]

سامية دخان[2]

كلية الآداب والعلوم الإنسانية والاجتماعية - جامعة الشارقة

الشارقة - الإمارات العربية المتحدة

ملخص البحث:

تُعدُّ وسائل التواصل الاجتماعي من أهم عوامل التحول الاجتماعي في العصر الحديث، إذ تؤدّي دوراً مهمًّا في حياة الملايين من الأشخاص، وخصوصاً عبر منصاتها، مثل: الفايسبوك والتويتر والانستغرام والسناب شات وغيرها الكثير، وذلك من خلال عرض آخر التحديثات في حياة الفرد والتواصل مع الأصدقاء وأفراد العائلة، فضلاً عن مشاركة الصور ومقاطع الفيديو الخاصة. وتساعد هذه المنصات في تواصل الملايين من الأشخاص، ومِن ثَمَّ فإن لها القدرة على التأثير على حياتهم بما في ذلك من تأثير سلبي لسوء الاستخدام. ويُتوقع من مستخدمي وسائل التواصل الاجتماعي استعمال هذه المنصات بشكل مسؤول؛ لأن الخصوصية ضرورية لتجنب الضرر والتشويه والكشف العلني والانتهاكات.

تبحث الدراسة في الخصوصية بوسائل التواصل الاجتماعي من منظور قانوني وأخلاقي في دولة الإمارات العربية المتحدة؛ إذ تعالج مخاوف المستخدمين الذين لا ينتبهون لموضوع الخصوصية عبر العالم الافتراضي، كما وتبحث في إرشادات حماية البيانات والفجوة في البحوث المرتبطة بالخصوصية على منصات التواصل الاجتماعي. وترتكز الدراسة على النظرية الأخلاقية النفعية الاجتماعية كإطار أخلاقي، فيما تُطبّق النظرية القانونية؛ لأنها تحدد وتضع حدوداً للخصوصية ومظاهرها المختلفة في وسائل التواصل الاجتماعي.

الوعي بالخصوصية هو عامل حاسم عند استخدام منصات التواصل الاجتماعي. لذلك، يجب أن يتحمل مقدمو هذه المنصات مسؤولية توجيه وتنوير المستخدمين لاتخاذ الحذر ومنع

(1) كلية الاتصال - جامعة الشارقة (الشارقة - الإمارات العربية المتحدة)

aazi@sharjah.ac.ae

(2) كلية الاتصال - جامعة الشارقة (الشارقة - الإمارات العربية المتحدة)

انتهاك الخصوصية على معلوماتهم الشخصية التي ينشرونها عبر هذه المواقع. تساعد نتائج هذه الورقة البحثية على توعية مستخدمي منصات التواصل لاتخاذ الاحتياطات والإجراءات اللازمة لحماية معلوماتهم وبياناتهم الخاصة، كما تشكل مرجعاً نظرياً للقائمين على هذه المنصات لمعرفة أهمية تثقيف المستخدمين عبر هذه المنصات لحماية بياناتهم الخاصة.

يُعِدُّ قانونُ الجرائمِ الإلكترونية (القانون الاتحادي رقم 5 لسنة 2012) في الإمارات العربية المتحدة، انتهاكَ الخصوصية عبر وسائل التواصل الاجتماعي جريمةً يُعاقِب عليها القانون، إذ تكون العقوبة ما بين السجن لمدة خمس سنوات وغرامة تتراوح بين 100,000 درهم و 500,000 درهم.

إن غالبية مستخدمي وسائل التواصل الاجتماعي غير مدركين لطرق حماية معلوماتهم الشخصية التي يتم مشاركتها عبر الإنترنت؛ إذ إنّ التكنولوجيا أصبحت أسهل ويمكن نشر صورة بضغطة زر واحدة، لكنهم يبقون غير مدركين لكيفية تأثير ذلك على حياتهم. وعلى الرغم من أن القائمين على وسائل التواصل الاجتماعي يعملون لتوفير أنظمة وميزات أساسية وأكثر أماناً، إلا أن الدور يبقى على المستخدم نفسه ومدى استعداده لتعلم كيفية استخدام هذه الميزات لحماية معلوماته الشخصية.

أظهرت هذه الدراسة أنه على الرغم من أنه لا يوجد إطار قانوني حصري عن الخصوصية في دولة الإمارات العربية المتحدة ولكن هناك العديد من القوانين ذات الصلة. لذلك، هناك حاجة لمزيد من استكشاف الخصوصية من قبل الجهات المسؤولة لوضع أبعاد قانونية جديدة في الدولة. ووفقاً لنتائج الدراسة من المنظور الأخلاقي، فإن أفراد عينة البحث ليس لهم الوعي الأخلاقي الكافي في التعامل مع موضوع الخصوصية على الشبكة.

وبينما لا يزال المنظور الأخلاقي مثيراً للجدل، فإن المنظور القانوني لخصوصية وسائل التواصل الاجتماعي في الإمارات العربية المتحدة يعتبر مرجعا في فهم الخصوصية من الناحية القانونية؛ لأنه يستند إلى العديد من القوانين التي تحمي المستخدمين، مثل قانون العقوبات الإماراتي، وقانون الجرائم الإلكترونية. ومع ذلك، تعتبر هذه القواعد أساساً للقوانين المستجدة التي تنشأ بسبب تطور أنظمة وسائل التواصل الاجتماعي في جميع أنحاء العالم.

الكلمات الدالة: الخصوصية، منصات التواصل الاجتماعي، النظرية الأخلاقية النفعية، النظرية القانونية